ABSTRACT OF THE DISCLOSURE

A cryptographic communications method based on ID-NIKS, wherewith mathematical structures are minimized, the collusion problem can be circumvented, and building the cryptosystem is simplified. A plurality of centers are provided for distributing a plurality of secret keys to a plurality of entities, respectively. Each secret key is unique to each entity. Information specifying the entities (entity ID information) is divided into a plurality of pieces or segments. All secret keys produced for the pieces of entity ID information are distributed to the entities. Using a component contained in the secret key peculiar to itself, each entity generates a common key to be shared by another entity. This component corresponds to a piece of ID information of another entity.